(F) ensure that all worker responses are confidential and are never shared with management; and

(G) interview a representative of the labor organization or other worker representative organization that represents workers at the facility or, if no such organization is present, attempt to interview a representative from a local worker advocacy group.

(2) MANAGEMENT INTERVIEWS.—The auditor shall—

(A) interview a cross-section of the management of the supplier, including human resources personnel, production supervisors, and others; and

(B) use audit tools to ensure that managers are asked a comprehensive set of questions.

(3) DOCUMENTATION REVIEW.—The auditor shall—

(A) conduct a documentation review to provide tangible proof of compliance and to corroborate or find discrepancies in the information gathered through the worker and management interviews; and

(B) review, at a minimum, the following types of documents:

(i) Age verification procedures and documents.

(ii) A master list of juvenile workers.

(iii) Selection and recruitment procedures.

(iv) Contracts with labor brokers, if any.

(v) Worker contracts and employment agreements.

(vi) Introduction program materials.

(vii) Personnel files.

(viii) Employee communication and training plans, including certifications provided to workers including skills training, worker preparedness, government certification programs, and systems or policy orientations.

(ix) Collective bargaining agreements, including collective bargaining representative certification, descriptions of the role of the labor organization, and minutes of the labor organization's meetings.

(x) Contracts with any security agency, and descriptions of the scope of responsibilities of the security agency.

(xi) Payroll and time records.

(xii) Production capacity reports.

(xiii) Written human resources policies and procedures.

(xiv) Occupational health and safety plans and records including legal permits, maintenance and monitoring records, injury and accident reports, investigation procedures, chemical inventories, personal protective equipment inventories, training certificates, and evacuation plans.

(xv) Disciplinary notices.

(xvi) Grievance reports.

(xvii) Performance evaluations.

(xviii) Promotion or merit increase records.

(xix) Dismissal and suspension records of workers.

(xx) Records of employees who have resigned.

(xxi) Worker pay stubs.

(4) CLOSING MEETING WITH MANAGEMENT.—The auditor shall hold a closing meeting with the management of the covered business entity to—

(A) report violations and nonconformities found in the facility; and

(B) determine the steps forward to address and remediate any problems.

(5) REPORT PREPARATION.—The auditor shall prepare a full report of the audit, which shall include—

(A) a disclosure of the direct supplier's or on-site service provider's—

(i) documented processes and procedures that relate to eradicating forced labor; and

(ii) documented risk assessment and prioritization policies as such policies relate to eradicating forced labor;

(B) a description of the worker interviews, manager interviews, and documentation review required under paragraphs (1), (2), and (3);

(C) a description of all violations or suspected violations by the direct supplier of any forced labor laws of the United States or, if applicable, the laws of another country as described in section 6132(b)(2)(B)(ii); and

(D) for each violation described in subparagraph (C), a description of any corrective and protective actions recommended for the direct supplier consisting of, at a minimum—

(i) the issues relating to the violation and any root causes of the violation;

(ii) the implementation of a solution; and

(iii) a method to check the effectiveness of the solution.

(b) ADDITIONAL REQUIREMENTS RELATING TO AUDITS.—Each covered business entity shall include, in any contract with a direct supplier or on-site service provider, a requirement that—

(1) the supplier or provider shall not retaliate against any worker for participating in an audit relating to forced labor; and

(2) worker participation in an audit shall be protected through the same grievance mechanisms available to the worker available for any other type of workplace grievance.

SEC. 6134. ENFORCEMENT.

(a) CIVIL DAMAGES.—The Secretary may assess civil damages in an amount of not more than $100,000,000 if, after notice and an opportunity for a hearing, the Secretary determines that a covered business entity has violated any requirement of section 6132(b).

(b) PUNITIVE DAMAGES.—In addition to damages under subsection (a), the Secretary may assess punitive damages in an amount of not more than $500,000,000 against a covered business entity if, after notice and an opportunity for a hearing, the Secretary determines the covered business entity willfully violated any requirement of section 6132(b).

(c) DECLARATIVE OR INJUNCTIVE RELIEF.—The Secretary may request the Attorney General institute a civil action for relief, including a permanent or temporary injunction, restraining order, or any other appropriate order, in the district court of the United States for any district in which the covered business entity conducts business, whenever the Secretary believes that a violation of section 6132(b) constitutes a hazard to workers.

SEC. 6135. REGULATIONS.

Not later than 180 days after the date of enactment of this Act, the Secretary shall promulgate rules to carry out this subtitle.

SA 1949. Mr. HAWLEY submitted an amendment intended to be proposed to amendment SA 1502 proposed by Mr. SCHUMER to the bill S. 1260, to establish a new Directorate for Technology and Innovation in the National Science Foundation, to establish a regional technology hub program, to require a strategy and report on economic security, science, research, innovation, manufacturing, and job creation, to establish a critical supply chain resiliency program, and for other purposes; which was ordered to lie on the table; as follows:

At the end of title V of division B, add the following:

SEC. 25___. PROHIBITION ON THE LICENSING AND TRANSFERRING OF CERTAIN INTELLECTUAL PROPERTY RIGHTS.

No intellectual property developed through research that is funded through the expenditure of Federal funds received under this division (or an amendment made by this division), or the appropriation of which are authorized under this division (or an amendment made by this division), may be licensed or transferred—

(1) to any business or research institution that is located outside of the United States; and

(2) for the commercialization or production of goods, services, or technologies.

SA 1950. Mr. HAWLEY submitted an amendment intended to be proposed to amendment SA 1502 proposed by Mr. SCHUMER to the bill S. 1260, to establish a new Directorate for Technology and Innovation in the National Science Foundation, to establish a regional technology hub program, to require a strategy and report on economic security, science, research, innovation, manufacturing, and job creation, to establish a critical supply chain resiliency program, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. _____. IMPOSING DATA SECURITY REQUIREMENTS AND STRENGTHENING REVIEW OF FOREIGN INVESTMENTS WITH RESPECT TO CERTAIN TECHNOLOGY COMPANIES FROM FOREIGN COUNTRIES OF CONCERN.

(a) DEFINITIONS.—In this section:

(1) COMMISSION.—The term ''Commission'' means the Federal Trade Commission.

(2) COUNTRY OF CONCERN.—

(A) IN GENERAL.—Subject to subparagraph (B)(iii), the term ''country of concern'' means—

(i) the People's Republic of China;

(ii) the Russian Federation; and

(iii) any other country designated by the Secretary of State as being of concern with respect to the protection of data privacy and security.

(B) DESIGNATION OF COUNTRIES OF CONCERN.—Not later than 1 year after the date of enactment of this Act, and annually thereafter, the Secretary of State shall—

(i) review the status of data privacy and security requirements (including by reviewing laws, policies, practices, and regulations related to data privacy and security) in each foreign country to determine—

(I) whether it would pose a substantial risk to the national security of the United States if the government of such country gained access to the user data of citizens and residents of the United States; and

(II) whether there is a substantial risk that the government of such country will, in a manner that fails to afford similar respect for civil liberties and privacy as the Constitution and laws of the United States, obtain user data from companies that collect user data;

(ii) designate each country that meets the criteria of clause (i) as a country of concern; and

(iii) remove the designation from any country that was previously designated a country of concern (regardless of whether such designation was pursuant to clause (i) or (ii) of subparagraph (A) or was made by the Secretary of State pursuant to clause (iii) of such subparagraph) if the country—

(I) no longer meets the criteria of clause (i); and

(II) is not at substantial risk of meeting such criteria.

(C) REGULATIONS.—Not later than 90 days after the date of the enactment of this Act, the Secretary of State shall prescribe regulations—

(i) establishing a process for a covered technology company or country of concern to petition the Secretary to remove the country of concern designation from a country that was designated as such pursuant to subparagraph (B)(ii); and

(ii) setting forth the procedures and criteria the Secretary will use in identifying or removing countries under subparagraphs (A)(iii) or (B)(iii).

(3) COVERED TECHNOLOGY COMPANY.—The term ''covered technology company'' means an entity that provides an online data-based service such as a website or internet application in or affecting interstate or foreign commerce and—

(A) is organized under the laws of a country of concern;

(B) in which foreign persons that are nationals of, or companies that are organized under the laws of, countries of concern have a plurality or controlling equity interest;

(C) is a subsidiary company of an entity described in subparagraph (A) or (B); or

(D) is otherwise subject to the jurisdiction of a country of concern in a manner that allows the country of concern to obtain the user data of citizens and residents of the United States without similar respect for civil liberties and privacy as provided under the Constitution and laws of the United States.

(4) FACIAL RECOGNITION TECHNOLOGY.—The term ''facial recognition technology'' means technology that analyzes facial features in still or video images and is used to identify, or facilitate identification of, an individual using facial physical characteristics.

(5) TARGETED ADVERTISING.—

(A) IN GENERAL.—The term ''targeted advertising'' means a form of advertising where advertisements are displayed to a user based on the user's traits, information from a profile about the user that is created for the purpose of selling advertisements, or the user's previous online or offline behavior.

(B) LIMITATION.—Such term shall not include advertising chosen because of the context of the internet service, such as—

(i) advertising that is directed to a user based on the content of the website, online service, online application, or mobile application that the user is connected to; or

(ii) advertising that is directed to a user by the operator of a website, online service, online application, or mobile application based on the search terms that the user used to arrive at such website, service, or application.

(6) USER DATA.—The term ''user data'' means any information obtained by an entity that provides a data-based service such as a website or internet application that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked with an individual who is a citizen or resident of the United States without regard to whether such information is directly submitted by the individual to the entity, is derived by the entity from the observed activity of the individual, or is obtained by the entity by any other means.

(b) DATA SECURITY REQUIREMENTS FOR COVERED TECHNOLOGY COMPANIES.—

(1) IN GENERAL.—The following requirements shall apply to a covered technology company:

(A) MINIMAL COLLECTION OF DATA.—The company shall not collect any more user data than is necessary for the operation of the website, service, or application of the company.

(B) PROHIBITION ON SECONDARY USES.—The company shall not use any user data collected under subparagraph (A) for any purpose that is secondary to the operation of the website, service, or application of the company, including providing targeted advertising, unnecessarily sharing such data with a third party, or unnecessarily facilitating facial recognition technology.

(C) RIGHT TO VIEW AND DELETE DATA.—The company shall allow an individual to—

(i) view any user data held by the company that relates to the individual; and

(ii) permanently delete any user data held by the company that has been collected, directly or indirectly, from the individual.

(D) PROHIBITION ON TRANSFER TO COUNTRIES OF CONCERN.—The company shall not transfer any user data or information needed to decipher that data, such as encryption keys, to any country of concern (including indirectly through a third country that is not a country of concern).

(E) DATA STORAGE REQUIREMENT.—The company shall not store any user data collected from citizens or residents of the United States or information needed to decipher that data, such as encryption keys, on a server or other data storage device that is located outside of the United States or a country that maintains an agreement with the United States to share data with law enforcement agencies through a process established by law.

(F) REPORTING REQUIREMENT.—Not less frequently than annually, the chief executive officer or equivalent officer of the company shall submit, under penalty of perjury, a report to the Commission, the Attorney General of the United States, and the Attorney General of each State certifying compliance with the requirements of this subsection.

(2) EXCEPTIONS.—

(A) EXCEPTION FOR LAW ENFORCEMENT AND MILITARY.—The requirements of subparagraphs (A) through (D) of paragraph (1) shall not apply where data is collected, used, retained, stored, or shared by a covered technology company solely for the purpose of assisting a law enforcement or military agency that is not affiliated with a country of concern.

(B) TRANSFER OF SHARED CONTENT.—The requirements of subparagraphs (E) and (F) of paragraph (1) shall not apply to user data that is content produced by a user for the purpose of sharing with other users (such as social media posts, emails, or data related to a transaction involving the user) or information needed to decipher that data provided that the transfer and any storage necessary to enact the transfer is conducted solely to carry out the user's intent to share such data with individual users in other countries and that necessary storage occurs only on the intended recipient's individual device.

(3) EFFECTIVE DATE.—The requirements of this subsection shall take effect 90 days after the date of enactment of this Act.

(c) DATA SECURITY REQUIREMENTS FOR OTHER TECHNOLOGY COMPANIES.—

(1) IN GENERAL.—The following requirements shall apply to any company operating in or affecting interstate or foreign commerce that provides a data-based service such as a website or internet application but is not a covered technology company:

(A) PROHIBITION ON TRANSFER TO COUNTRIES OF CONCERN.—The company shall not transfer any user data collected from an individual in the United States or information needed to decipher that data, such as encryption keys, to any country of concern (including indirectly through a third country that is not a country of concern).

(B) PROHIBITION ON STORING DATA IN COUNTRIES OF CONCERN.—The company shall not store any user data collected from an individual in the United States or information needed to decipher that data, such as encryption keys, on a server or other data storage device that is located in any country of concern.

(2) EXCEPTIONS.—

(A) EXCEPTION FOR LAW ENFORCEMENT AND MILITARY.—The requirements of paragraph (1) shall not apply where data is collected, used, retained, stored, or shared by a covered technology company solely for the purpose of assisting a law enforcement or military agency that is not affiliated with a country of concern.

(B) TRANSFER OF SHARED CONTENT.—The requirements of paragraph (1) shall not apply to user data that is content produced by a user for the purpose of sharing with other users (such as social media posts, emails, or data related to a transaction involving the user) or information needed to decipher that data provided that the transfer and any storage necessary to enact the transfer is conducted solely to carry out the user's intent to share such data with individual users in other countries and that necessary storage occurs only on the intended recipient's individual device.

(3) EFFECTIVE DATE.—The requirements of this subsection shall take effect 90 days after the date of enactment of this Act.

(d) ENFORCEMENT OF DATA SECURITY REQUIREMENTS.—

(1) ENFORCEMENT BY THE COMMISSION.—

(A) IN GENERAL.—Except as otherwise provided, subsections (b) and (c) shall be enforced by the Commission under the Federal Trade Commission Act (15 U.S.C. 41 et seq.).

(B) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—A violation of subsection (b) or (c) shall be treated as a violation of a rule defining an unfair or deceptive act or practice prescribed under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)).

(C) ACTIONS BY THE COMMISSION.—Except as otherwise provided, the Commission shall prevent any person from violating subsection (b) or (c) in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this section, and any person who violates such a subsection shall be subject to the penalties and entitled to the privileges and immunities provided in the Federal Trade Commission Act.

(D) AUTHORITY PRESERVED.—Nothing in this section shall be construed to limit the authority of the Commission under any other provision of law.

(2) CRIMINAL PENALTY.—

(A) OFFENSE.—It shall be unlawful to knowingly cause a technology company to violate a requirement of subsection (b) or (c).

(B) PENALTY.—Any person who violates subparagraph (A) shall be imprisoned for not more than 5 years, fined under title 18, United States Code, or both.

(3) ENFORCEMENT BY STATE ATTORNEYS GENERAL.—

(A) IN GENERAL.—

(i) CIVIL ACTIONS.—In any case in which the attorney general of a State has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by the engagement of any person in a practice that violates subsection (b) or (c), the State, as parens patriae, may bring a civil action on behalf of the residents of the State in a district court of the United States or a State court of appropriate jurisdiction to—

(I) enjoin that practice;

(II) enforce compliance with such section;

(III) on behalf of residents of the State, obtain damages, statutory damages, restitution, or other compensation, each of which shall be distributed in accordance with State law; or

(IV) obtain such other relief as the court may consider to be appropriate.

(ii) NOTICE.—

(I) IN GENERAL.—Before filing an action under clause (i), the attorney general of the State involved shall provide to the Commission—

(aa) written notice of that action; and

(bb) a copy of the complaint for that action.

(II) EXEMPTION.—

(aa) IN GENERAL.—Subclause (I) shall not apply with respect to the filing of an action by an attorney general of a State under this subparagraph if the attorney general of the State determines that it is not feasible to provide the notice described in that subclause before the filing of the action.

(bb) NOTIFICATION.—In an action described in item (aa), the attorney general of a State shall provide notice and a copy of the complaint to the Commission at the same time as the attorney general files the action.

(B) INTERVENTION.—

(i) IN GENERAL.—On receiving notice under subparagraph (A)(ii), the Commission shall have the right to intervene in the action that is the subject of the notice.

(ii) EFFECT OF INTERVENTION.—If the Commission intervenes in an action under subparagraph (A), it shall have the right—

(I) to be heard with respect to any matter that arises in that action; and

(II) to file a petition for appeal.

(C) CONSTRUCTION.—For purposes of bringing any civil action under subparagraph (A), nothing in this section shall be construed to prevent an attorney general of a State from exercising the powers conferred on the attorney general by the laws of that State to—

(i) conduct investigations;

(ii) administer oaths or affirmations; or

(iii) compel the attendance of witnesses or the production of documentary and other evidence.

(D) ACTIONS BY THE COMMISSION.—In any case in which an action is instituted by or on behalf of the Commission for violation of subsection (b) or (c), no State may, during the pendency of that action, institute an action under subparagraph (A) against any defendant named in the complaint in the action instituted by or on behalf of the Commission for that violation.

(E) VENUE; SERVICE OF PROCESS.—

(i) VENUE.—Any action brought under subparagraph (A) may be brought in—

(I) the district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28, United States Code; or

(II) a State court of competent jurisdiction.

(ii) SERVICE OF PROCESS.—In an action brought under subparagraph (A) in a district court of the United States, process may be served wherever defendant—

(I) is an inhabitant; or

(II) may be found.

(4) PRIVATE RIGHT OF ACTION.—

(A) IN GENERAL.—Any individual who suffers injury as a result of an act, practice, or omission of a covered technology company that violates subsection (b) may bring a civil action against such company in any court of competent jurisdiction.

(B) RELIEF.—In a civil action brought under subparagraph (A) in which the plaintiff prevails, the court may award such plaintiff up to $1,000 for each day that such plaintiff was affected by a violation of subsection (b) (up to a maximum of $15,000 per each such violation per plaintiff).

(e) REQUIREMENT FOR APPROVAL OF COMMITTEE ON FOREIGN INVESTMENT IN THE UNITED STATES OF CERTAIN TRANSACTIONS.—Section 721(b) of the Defense Production Act of 1950 (50 U.S.C. 4565(b)) is amended by adding at the end the following:

''(9) APPROVAL REQUIRED FOR CERTAIN TRANSACTIONS.—

''(A) IN GENERAL.—A covered transaction described in subparagraph (C) is prohibited unless the Committee—

''(i) reviews the transaction under this subsection; and

''(ii) determines that the transaction does not pose a risk to the national security of the United States.

''(B) MITIGATION.—The Committee, or a lead agency on behalf of the Committee, may negotiate, enter into or impose, and enforce an agreement or condition under subsection (l)(3) with any party to a covered transaction described in subparagraph (C) to mitigate any risk to the national security of the United States that arises as a result of the covered transaction.

''(C) COVERED TRANSACTION DESCRIBED.—A covered transaction described in this subparagraph is a transaction that could result in foreign control of a United States company—

''(i) that collects, sells, buys, or processes user data and whose business consists substantially more of transferring data than manufacturing, delivering, repairing, or servicing physical goods or providing physical services; or

''(ii) that operates a social media platform or website.

''(D) USER DATA DEFINED.—For purposes of subparagraph (C), the term 'user data' means any information obtained by an entity that provides a data-based service such as a website or internet application that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked with an individual who is a citizen or resident of the United States without regard to whether such information is directly submitted by the individual to the entity, is derived by the entity from the observed activity of the individual, or is obtained by the entity by any other means.''.

SA 1951. Mr. HAWLEY submitted an amendment intended to be proposed to amendment SA 1502 proposed by Mr. SCHUMER to the bill S. 1260, to establish a new Directorate for Technology and Innovation in the National Science Foundation, to establish a regional technology hub program, to require a strategy and report on economic security, science, research, innovation, manufacturing, and job creation, to establish a critical supply chain resiliency program, and for other purposes; which was ordered to lie on the table; as follows:

In title III of division C, insert after section 3302 the following:

SEC. 3303. MEASURES TO PREVENT IMPORTATION OF GOODS MADE WITH FORCED LABOR.

(a) DUTIES ON IMPORTS FROM XINJIANG.—

(1) IN GENERAL.—During the period specified in paragraph (2), there shall be imposed a duty of 100 percent ad valorem, in addition to all duties otherwise applicable, on all goods, wares, articles, or merchandise—

(A) mined, produced, or manufactured wholly or in part in the Xinjiang Uyghur Autonomous Region of the People's Republic of China; or

(B) manufactured or assembled from any component part or material that is mined, produced, or manufactured in the Xinjiang Uyghur Autonomous Region.

(2) PERIOD SPECIFIED.—The period specified in this paragraph is the period—

(A) beginning on the date that is 90 days after the date of the enactment of this Act; and

(B) ending on the date, which may not be before the date that is one year after such date of enactment, on which the Secretary of State, in consultation with the Secretary of Labor, the Commissioner of U.S. Customs and Border Protection, and the United States Trade Representative—

(i) determines beyond a reasonable doubt that no slave labor, forced labor, indentured labor, or child labor exists in the People's Republic of China; and

(ii) submits to Congress and makes available to the public a report on that determination.

(3) REGULATIONS.—The Commissioner of U.S. Customs and Border Protection may prescribe regulations necessary for the enforcement of paragraph (1).

(b) INELIGIBILITY OF COUNTRIES THAT USE FORCED LABOR FOR GENERALIZED SYSTEM OF PREFERENCES.—

(1) IN GENERAL.—Section 502(b)(2) of the Trade Act of 1974 (19 U.S.C. 2462(b)(2)) is amended—

(A) by inserting after subparagraph (H) the following:

''(I) Such country is identified by the Bureau of International Labor Affairs of the Department of Labor pursuant to section 105(b)(2)(C) of the Trafficking Victims Protection Reauthorization Act of 2005 (22 U.S.C. 7112(b)(2)(C)) as a source country of goods that are believed to be produced by forced labor or child labor in violation of international standards.''; and

(B) in the flush text at the end, by striking ''(F),'' and all that follows through ''section 507(6)(D))'' and inserting ''and (F)''.

(2) EFFECTIVE DATE.—The amendments made by paragraph (1) apply with respect to articles entered on or after the date that is 30 days after the date of the enactment of this Act.

SA 1952. Mr. HAWLEY submitted an amendment intended to be proposed to amendment SA 1502 proposed by Mr. SCHUMER to the bill S. 1260, to establish a new Directorate for Technology and Innovation in the National Science Foundation, to establish a regional technology hub program, to require a strategy and report on economic security, science, research, innovation, manufacturing, and job creation, to establish a critical supply chain resiliency program, and for other purposes; which was ordered to lie on the table; as follows:

In division B, insert after section 2510 the following:

SEC. 2511. MARKING OF ARTICLES THAT ORIGINATE IN COUNTRIES BELIEVED TO PRODUCE GOODS MADE BY FORCED LABOR OR CHILD LABOR.

(a) IN GENERAL.—It shall be unlawful for an article that is required to be marked under section 304 of the Tariff Act of 1930 (19 U.S.C. 1304) and originates in a source country to be introduced, sold, advertised, or offered for sale in commerce in the United States unless that article is legibly, indelibly, and permanently marked, in addition to being marked with the English name of the country of origin of the article as required by such section 304, as follows: ''The United States Department of Labor has reason to believe that goods from this country are produced by child labor or forced labor in violation of international standards.''.

(b) ADDITIONAL DUTIES; DELIVERY WITHHELD; PENALTIES.—The provisions of subsections (i), (j), and (l) of section 304 of the Tariff Act of 1930 (19 U.S.C. 1304) apply with respect to an article that is not marked as required by subsection (a) to the same extent